Notice of Allowability	**Application No.** 09/905,341	**Applicant(s)** YANN ET AL.	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *September 15, 2005*.

2. ☒ The allowed claim(s) is/are *1-5,8-16,18 and 20-33*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Samir A. Bhavsar on 2/15/06.

2. The application has been amended as follows:

In claim 1

"detecting at least one unused or misused operand or operator of the first predetermined number of instructions;

collecting information corresponding to a plurality of registers and/or flags after emulating at least one instruction;"

has been changed to

--detecting at least one unused or misused operand or operator of the first predetermined number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one operand or operator that is not used during emulation of the first predetermined number of instructions;

collecting information after emulating at least one instruction, wherein at least a portion of the collected information corresponds to a plurality of registers and/or flags and to the at least one detected unused or misused operand or operator; --

In claim 7

"(Currently Amended)"

has been changed to

--(Canceled)--

In claim 8

"(Currently Amended) The method of claim 1, wherein detecting at least one unused or misused operand or operator comprises identifying at least one undefined operand or operator used during emulation of the first predetermined number of instructions."

has been changed to

--(Currently Amended) A method of detecting polymorphic viral code, comprising:

emulating a first predetermined number of instructions of a computer program;

detecting at least one unused or misused operand or operator of the first predetermined number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one undefined operand or operator used during emulation of the first predetermined number of instructions;

collecting information after emulating at least one instruction, wherein at least a portion of the collected information corresponds to a plurality of registers and/or flags and to the at least one detected unused or misused operand or operator; and

determining a probability that the computer program contains polymorphic viral code based at least in part on an heuristic analysis of the collected information.—

In claim 9

"detecting at least one unused or misused operand or operator of the selected number of instructions;

collecting information corresponding to a plurality of registers and/or flags after emulating at least one instruction;"

has been changed to

--detecting at least one unused or misused operand or operator of the selected number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one operand or operator that is not used during emulation of the selected number of instructions;

collecting information after emulating at least one instruction, wherein at least a portion of the collected information corresponds to a plurality of registers and/or flags and to the at least one detected unused or misused operand or operator; --

In claim 10

"detecting at least one unused or misused operand or operator of the selected number of instructions;

collecting and storinginformation corresponding to a plurality of registers and/or flags after emulating at least one instruction;"

has been changed to

--detecting at least one unused or misused operand or operator of the selected number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one undefined operand or operator used during emulation of the selected number of instructions;

collecting and storing information after emulating at least one instruction, wherein at least a portion of the collected information corresponds to a plurality of registers and/or flags and to the at least one detected unused or misused operand or operator; --

In claim 11

"a second segment including detection code to detect at least one unused or misused operand or operator of the selected number of instructions;"

has been changed to

--a second segment including detection code to detect at least one unused or misused operand or operator of the selected number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one operand or operator that is not used during emulation of the selected number of instructions;--

"a fourth segment including heuristic processor code to determine a probability that the computer program contains polymorphic viral code based at least in part on an heuristic analysis of the plurality of registers and/or flags."

has been changed to

-- a fourth segment including heuristic processor code to determine a probability that the computer program contains polymorphic viral code based at least in part on an heuristic analysis of the plurality of registers and/or flags and the at least one detected unused or misused operand or operator.--

In claim 12

“detect at least one unused or misused operand or operator of the first predetermined number of instructions;”

has been changed to

--detect at least one unused or misused operand or operator of the first predetermined number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one undefined operand or operator used during emulation of the first predetermined number of instructions;--

“an heuristic analyzer operable to determine a probability that the computer program contains polymorphic viral code based at least in part on an heuristic analysis of the plurality of registers and/or flags.”

has been changed to

--an heuristic analyzer operable to determine a probability that the computer program contains polymorphic viral code based at least in part on an heuristic analysis of the plurality of registers and/or flags and the at least one detected unused or misused operand or operator.--

In claim 18

“The apparatus of claim 12, wherein detecting at least one unused or misused operand or operator comprises identifying at least one undefined operand or operator used during emulation of the first predetermined number of instructions.”

has been changed to

--An apparatus for detecting polymorphic viral code, comprising:

an emulator operable to emulate a first predetermined number of instructions of a computer program;

an operational code analyzer operable to:

detect at least one unused or misused operand or operator of the first predetermined number of instructions, wherein detecting at least one unused or misused operand or operator comprises identifying at least one operand or operator that is not used during emulation of the first predetermined number of instructions; and

analyze a plurality of registers and/or flags accessed during emulation of at least one instruction;

and

an heuristic analyzer operable to determine a probability that the computer program contains polymorphic viral code based at least in part on an heuristic analysis of the plurality of registers and/or flags and the at least one detected unused or misused operand or operator.--

In claim 19

"(Currently Amended)"

has been changed to

--(Canceled)—

In claim 25

"(New) The method of claim 7"

has been changed to

--(Currently Amended) The method of claim 1—

In claim 27

"generate or modifying at least one rule based on at least in part on the identification of the polymorphic viral code."

has been changed to

--generate or modify at least one rule based on at least in part on the identification of the polymorphic viral code.—

In claim 31

"(New) The method of claim 16, wherein the heuristic analysis comprises comparing the number of time that the register and/or flag was improperly used with statistics corresponding to a plurality of polymorphic viral codes."

has been changed to

--(Currently Amended) The method of claim 16, wherein the heuristic analysis comprises comparing the number of times that the register and/or flag was improperly used with statistics corresponding to a plurality of polymorphic viral codes.--

In claim 33

"(New) The method of claim 19,"

has been changed to

--(Currently Amended) The method of claim 12,--

Allowable Subject Matter

3. This action is in response to the communication dated September 15, 2005.

4. Claims 15, 8-16, 18 and 20-33 are allowed.

5. The following is an examiner's statement of reasons for allowance:

The present invention is directed to a method and apparatus for detecting polymorphic viral code in a computer program. Each independent claim (claims 1, 8, 9, 10, 11, 12 and 18) identifies the uniquely distinct features of identifying at least one operand or operator that is not used during emulation of the selected number of instructions when detecting at least one unused or misused operand or operator and identifying at least one undefined operand or operator used during emulation of the selected number of instructions when detecting at least one unused or misused operand or operator. The closest prior arts, Nachenberg et al. (5,826,013), (5,964,889) and (6,357,008) fail to anticipate or render the above limitations obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
2/15/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER